REMARKS

This responds to the Office Action mailed on April 14, 2006.

Claims 17, 21, 25-28 and 30-33 are amended, claim 24 and 34 are canceled, and no claims are added; as a result, claims 4, 5, 7-13, 16-23, and 25-33 are now pending in this application.

§112 Rejection of the Claims

Claims 24-27 and 31-34 were rejected under 35 U.S.C. § 112, first paragraph, as lacking adequate description or enablement. The claims have been amended to address this issue.

§103 Rejection of the Claims

Claims 4-5, 7-9, 18, 21, and 28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ying et al. (U.S. 6,853,980) and Krueger et al. (U.S. 2002/0077837).

Ying describes a method and apparatus where an end user authentication method is done at one server (Col. 23, Fig.1 Font e-Commerce Server) using a username and a password, and the end user's card information is approved at different server (Col. 23, line 52-64, Fig.1 Credit Card Processor).

Krueger describes a method and apparatus where an end user's card information is verified at a central security server located in a web site different from a merchant's web site (¶¶ 40, 43-44, Fig. 2-7).

In contrast to Ying and Krueger, Applicant teaches that strong authentication requires authentication based on at least two factors associated with a user: what the user knows (e.g., a password), what the user has (e.g., a token) and a characteristic of the user (e.g., a fingerprint or retinal scan).

Neither Ying or Krueger, alone or in combination, teach or suggest an authentication method or apparatus that uses two or more authenticating factors associated with a user as taught by Applicant and claimed in claims 4-5, 7-13 and 16-34.

As indicated by the Examiner (Office Action, p. 4, No. 14), Ying uses user name and password (one factor) for the first authentication at the first server. Once the first authentication is done, both Ying and Krueger send the user's credit card information to the second server located in a different web site. (Col. 23, Fig. 1) (¶ 40-44). Under either Ying or Krueger's approach, however, the second system or method just checks the validity of the card information without verifying the card holder's identity.

In addition, both Ying and Krueger use single factor information of the same type for an increased secured transaction. Like the username or password, the end user's card information is also 'what the end user knows'. The card information is not 'what the end user has' such as a token-generated synchronous code enabling the card information processing server to authenticate the identity of the end user. Therefore, Ying or Krueger, alone or in combination, does not teach or suggest a method and apparatus for authentication using two factors as described and claimed by Applicant.

Claims 21 and 28 have been amended to emphasize this difference. Reconsideration is respectfully requested.

Claims 10-12, 19-20, 22-27, and 29-34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ying et al. (U.S. 6,853,980) and Krueger et al. (U.S. 2002/0077837), as applied to claims 21 and 28 above, in further view of "RSA Web Security Portfolio, How RSA SecurID Agents Can Secure Your Website" by RSA.

Claims 10-12, 19-20, 22-23, 25-27, and 29-33 are, however, patentable as depending on a patentable base claim. In addition, with regard to claims 23, 27, 31 and 33, none of the Ying, Krueger in further view of RSA, alone or in combination, teach or suggest an one-time password encrypted using a public key infrastructure as described and claimed by Applicant.

Claim 13 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Ying et al. (U.S. 6,853,980), Krueger et al. (U.S. 2002/0077837), and RSA as applied to claim 11 above, in further view of Tan et al. (U.S. Patent Application (U.S. 2001/0045451) in further view of "eToken: The Key to Security for the Internet Age" by Aladdin".

Claims 13 is, however, patentable as depending on a patentable base claim.

Claims 16-17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ying et al. (U.S. 6,853,980), Krueger et al. (U.S. 2002/0077837), and RSA, as applied to claim 4 above, in further view of Network Security Essentials Applications and Standards by Stallings.

Claims 16-17 are, however, patentable as depending on a patentable base claim. In addition, with regard to claim 17, Ying and Krueger, alone or in combination, do not teach or suggest an one-time password encrypted using a public key infrastructure as described and claimed by Applicant. Claim 17 has been amended to emphasize this difference. Reconsideration is respectfully requested.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (612) 373-6909 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

SEAN BRENNAN

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6909

Date July 14, 2006 By Thomas F. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 14th day of May, 2006.

Amy Moriarty
Name

Signature